EXHIBIT A

Committee on Consumer Affairs and Business Licensing
Balqees Mihirig, *Senior Counsel*
Leah Skrzypiec, *Policy Analyst*
Noah Meixler, *Policy Analyst*
Jeanne Florentine Kabore, *Finance Analyst*

THE COUNCIL OF THE CITY OF NEW YORK

COMMITTEE REPORT OF
THE GOVERNMENTAL AFFAIRS DIVISION
Jeffrey Baker, Legislative Director
Rachel Cordero, Deputy Director, Governmental Affairs

COMMITTEE ON CONSUMER AFFAIRS AND BUSINESS LICENSING
Hon. Andrew Cohen, Chair

December 10, 2020

INT. NO. 1170-A:	By Council Members Torres, Rosenthal, Rivera, Moya, Rose, Cornegy, Louis, Gibson, Kallos, Menchaca and Ayala
TITLE:	A Local Law to amend the administrative code of the city of New York, in relation to requiring businesses to notify customers of the use of biometric identifier technology and prohibiting the sale of biometric identifier information

I. INTRODUCTION

On December 10, 2020, the Committee on Consumer Affairs and Business Licensing, chaired by Council Member Andrew Cohen, held a remote vote on Proposed Int. No. 1170-A, in relation to requiring businesses to notify customers of the use of biometric identifier technology, and prohibiting the sale of biometric identifier information. The Committee heard testimony on a previous version of this bill at a joint hearing in October 2019, where the Departments of Information Technology and Telecommunications, and Consumer and Worker Protection, chambers of commerce, advocacy groups, community-based non-profit organizations, and other interested members of the public provided feedback on this bill. At the vote on December 10, the Committee voted 6 in favor, 0 opposed and 0 abstentions on the bill.

II. BACKGROUND

Biometric and Facial Recognition Technology

As with all technology, that used to identify individuals is rapidly evolving, and used for a variety of both security and for-profit purposes. Biometric identification techniques have expanded from simply revealing basic physical attributes to now include fingerprint, iris and retinal scans, voice recognition, DNA tests, and facial recognition.[1] Additionally, biometric identification methods are expanding in real-time to include measures, such as brain signal identification, and heart pattern and finger vein pattern recognition.[2]

[1] Center for Global Development, *Biometrics FAQs*, CGD, 2019, available at: https://www.cgdev.org/page/biometrics-faqs.
[2] Li, Cha and Tappert *Biometric Distinctiveness of Brain Signals Based on EEG*, 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, pp. 1-6 (2018); R. Palaniappan, and S. M. Krishnan, *Identifying individuals using ECG signals*, Proceedings of International Conference on Signal Processing and Communications, Bangalore, India, pp. 569–572, 11–14 (2004); Mulyono, David & Horng, Shi-Jinn. A study of finger vein biometric for personal identification (2008).

Typically, there are two main classes of biometrics data that can be collected in order to identify an individual: (1) behavioral characteristics; and (2) physiological characteristics.[3] Behavioral characteristics concern the behavior of an individual, while physiological characteristics concern the shape or composition of the body. Behavioral biometrics include an individual's keystroke, signature and voice recognition.[4] Physiological biometrics include facial recognition, fingerprint and iris scanning, hand geometry, and DNA.[5] Facial recognition systems use an individual's physiological information such as facial structure, eye color, size and shape.[6]

Facial recognition technology can identify an individual from a digital image by comparing and analyzing facial patterns.[7] This technology can also compare live captures of individuals or their digital image data to the record of the individual that is stored in the database.[8] Facial recognition technology involves scanning a particular area. Person's faces within a 35-degree angle of the camera can be extracted from the people in the monitored area.[9] Rapidly, facial characteristics, or nodal points, may be identified and recorded. Nodal points include such characteristics as depth of eye sockets, distance between eyes, and width of nose. Once these points have been identified, the nodal point measurements are turned into a comprehensive numerical code, which is called a faceprint. Within a minute, millions of faceprints can be compared to a

[3] Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. Marshall L. Rev. 589, 589–92 (2018) (citing Margaret Rouse, Biometrics, www.searchsecurity.techtarget.com/definition/biometrics; *see* generally What is Biometrics?, IDEMIA, www.morpho.com/en/biometrics)
[4] Id.
[5] Id.
[6] Id.
[7] Tarun Agarwal, *Biometric Sensors—Types and Its Workings*, ELPROCUS, www.elprocus.com/different-types-biometric-sensors/.
[8] *See supra*, note 3.
[9] Kanya A. Bennett, *Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveillance Systems*, 3 N.C. J.L. & Tech. 151 (2001) (citing Kevin Bonsor, *How Facial Recognition Works*, at http://www.howstuffworks.com/facial-recognition.htm).

database of stored faceprints.[10] Different facial recognition systems use slightly different methods.[11]

Facial recognition technology allows for: (1) facial classification, by classifying the face into categories such as an estimation of gender, age or race; (2) verification, by comparing the similarity of previously stored faceprint of any particular individual to a new faceprint and establishing a confidence score that the two individuals are the same; and (3) identification, by comparing a person's facial image to a database of stored faceprints.[12]

The Use of Facial Recognition Technologies

Retail Sector

Facial recognition is a rapidly growing biometric technology used in the retail sector.[13] From a business and marketing perspective, facial recognition is viewed as an important tool in the toolbox of "the future of shopping," with retailers readily experimenting with its potential. For example, services such as FaceFirst offer facial recognition technology specifically targeted towards retailers using "surveillance...and an underlying software platform that leverages artificial intelligence to [prevent] theft, [fraud,]...and...violence." [14] FaceFirst can scan faces as far as 50 to

[10] Id.
[11] Id.
[12] Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 621 (2019) (citing Federal Trade Commission, Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies, 4-5 (2012)).
[13] A recent study found that facial recognition is likely to generate revenue of $9.78 billion by 2023, growing at a compounded annual growth rate of 16.81% between 2017 and 2023; *Global Facial Recognition Market Report 2018*, Cision: PR Newswire (June 5, 2018), https://www.prnewswire.com/news-releases/global-facial-recognition-market-report-2018-300660163.htm; Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 685 (2019).
[14] Nick Coult, *Facial Recognition Software: Coming Soon to Your Local Retailer?*, Crime Rep. (Apr. 23, 2018), https://thecrimereport.org/2018/04/23/facial-recognition-software-coming-soon-to-your-local-retailer; Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 685 (2019).

100 feet away.[15] When a person walks through a store's entrance, a video camera captures multiple images of the shopper, selects the clearest one and adds the shopper's picture to the store's client database.[16] FaceFirst software compares that image with other images in its database. If a match occurs, either recognizing the shopper as a suspected shoplifter or important client, the software can alert store employees within seconds of the person's entrance into the store. After being added to the database, the software can recognize the customer on each subsequent visit to the store. Similarly, retailers can pre-set pictures of individuals they wish to track in the system such as individuals suspected of burglaries based on information from nearby stores or police records.[17]

In 2015, Walmart tested a system that scanned the faces of all individuals entering several of its stores; the system could identify suspected shoplifters, and instantly alert store security on their mobile devices.[18] Target is another large retailer that tested facial recognition software, "in a small number of Target stores to understand its ability to help prevent fraud and theft."[19] In March of 2018, the American Civil Liberties Union (ACLU) reached out to 20 of the biggest stores in the

[15] *See* Chris Burt, *FaceFirst Facial Recognition Coming to Thousands of U.S. Retail Locations*, Biometric Update, Aug. 21, 2018, https://www.biometricupdate.com/201808/facefirst-facial-recognition-coming-to-thousands-of-u-s-retail-locations; Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 569 (2019).

[16] *See* David Lumb, *Is Facial Recognition The Next Privacy Battleground?*, Fast Co. , Jan. 26, 2015, http://www.fastcompany.com/3040375/is-facial-recognitionthenext-privacy-battleground; Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 569 (2019).

[17] Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 543–44 (2019).

[18] Chris Frey, *Revealed: How Facial Recognition Has Invaded Shops--and Your Privacy*, The Guardian, (Mar. 3, 2016), https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto; *see also* Sapna Maheshwari, *Stores See a Future Without "May I Help You?" (They'll Already Have Your Data),* N.Y. Times (Mar. 10, 2019), https://www.nytimes.com/2019/03/10/business/retail-stores-technology.html; Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 685 (2019).

[19] Jenna Reck, a Target spokesperson, Leticia Miranda, *Thousands of Stores Will Soon Use Facial Recognition*, *And They Won't Need Your Consent*, BuzzFeedNews, August 17, 2018, https://www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at.

United States to ask if they use facial recognition technology: the resulting report stated that "of the 20 companies...contacted, only one was willing to tell [the ACLU] that they don't use it."[20]

Although many facial recognition products presently on the market focus on increasing security, customer engagement and marketing capabilities might be the true value for some retailers in the future. Facial recognition can be used by retailers to connect online with offline behaviors,[21] provide more in-depth market demographics and track in-store product engagement. With this omnichannel approach, retailers can track "aggregated bits of data collected through loyalty programs, point of sale records and other sources."[22]

Further, by using multiple tracking technologies, retailers might manipulate the availability, cost and appeal of an item.[23] This type of pricing, in part, uses existing customer information to determine the ideal cost that a shopper will spend on a particular item. Consumers provide retailers with this information "whenever they make a credit card purchase[,]...use free e-mail services, surf [the Internet] for information[,] or engage in social media."[24] Moreover, retailers can purchase the data obtained by social media platforms, such as shoppers' e-mail addresses and other personal information.[25] This information enables retailers "to develop a broad

---

[20] *Are Stores You Shop at Secretly Using Face Recognition on You?* March 28, 2019, ACLU, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/are-stores-you-shop-secretly-using-face.
[21] This approach is called omnichannel.
[22] *See supra*, note 18.
[23] Stephanie Pandolph, *Shoppers Expect More Personalization*, Bus. Insider, Oct. 26, 2017, https://www.businessinsider.com/shoppers-expect-more-personalization-2017-10; Victoria Greene, *7 Examples of Big Data Personalization*, Big Data, Oct. 11, 2018, https://bigdata-madesimple.com/7-examples-of-big-data-retail-personalization/; Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 569 (2019).
[24] Akiva A. Miller, *What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing*, 19 J. Tech. L. & Pol'y 43, 91 (2014); Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 569 (2019).
[25] Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 569 (2019); Seth Schoen, *New Cookie Technologies: Harder to See and Remove, Widely Used to Track You*, Elec. Frontier Found, Sept. 14, 2009, https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide.

picture about a consumer, such as identifying that the individual owns a house, runs marathons, eats healthy food, has a premium bank card, and is good in financial health."[26]

Entertainment Venues

The use of facial recognition technology at entertainment venues dates to at least the early 2000s. In January 2001, facial recognition technology was installed at the Raymond James Stadium by the Tampa Police Department to scan the faces of Super Bowl attendees.[27] Since then, this technology has proliferated and is now used at several entertainment venues, including Madison Square Gardens and Barclays Center.[28] In 2018, Live Nation and Ticketmaster invested in Blink Identity, a company that specializes in military-grade facial recognition software.[29]

The details surrounding how this technology will be used are closely guarded, but venues claim that the technology is needed for security and operational purposes to determine who may enter the premises.[30] For example, some artists, like Taylor Swift, reportedly use this technology at concerts to track stalkers.[31] Venues also use this technology to identify employees and vendors.[32] In Brooklyn, the Barclays Center has teamed up with IDEMIA, which manages the Transportation Security Administration's PreCheck program, to offer expedited entry lines.[33] Similarly, Live Nation claims that they intend to use the technology to improve the customer experience by linking tickets to faces and offering tailored services.[34]

---

[26] Id.
[27] Robert H. Thornburg, *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment*, 20 J. Marshall J. Computer & Info. L. 321 (Winter 2002).
[28] Kevin Draper "Madison Square Garden Has Used Face-Scanning Technology on Customers", *New York Times,* March 13, 2018, available at: https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html.
[29] Maggie Serota "Ticketmaster Explores Replacing Tickets With Facial Recognition"*, Spin Magazine*, May 8, 2018, available at: https://www.spin.com/2018/05/ticketmaster-facial-recognition-blink-live-nation/.
[30] *See supra,* note 28.
[31] Steven Knopper "Why Taylor Swift Is Using Facial Recognition at Concerts", *Rolling Stone*, December 13, 2018, available at: https://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741/.
[32] *See supra,* note 28.
[33] Id.
[34] *See supra,* note 29.

It is unclear how the data collected through facial recognition technology is managed and stored by entertainment venues. Facial recognition technology can often determine the age range and likely gender of concertgoers.[35] Technology experts warn that this data could be collected and sold to third parties for marketing purposes without the consent of consumers.[36] Several artists and activists have begun to speak out on the use of the technology. Fight For the Future, a nonprofit digital rights group, is campaigning to ban facial recognition software as a law enforcement tool, and recently launched a campaign against the use of the technology at concerts and festivals.[37] Tom Morello, of Rage Against the Machine, Amanda Palmer, Downtown Boys, Anti-Flag, and others have spoken up in support of the campaign.[38] Some musicians have expressed concerns that the technology will be used to target undocumented immigrants.[39] In response, several music festivals (including the Governor's Ball, in New York City, Bonnaroo in Tennessee, Punk Rock Bowling, in Las Vegas, Electric Forest in Michigan and Austin City Limits) announced they would cease using the technology.[40]

Casinos

Notably, casinos began using facial recognition technology years ago.[41] The technology was introduced as far back as 1994 at the Bally's Las Vegas Hotel and Casino in Las Vegas,

---

[35] *See supra,* note 29.
[36] Wendy Mesley "The Weekly Briefing: Interview with Takara Small" *CBC News*, May 20, 2018, available at: https://www.youtube.com/watch?v=6lpHzPMcAI0.
[37] Amanda Gersten "Musicians and Activists Speak Out Against Ticketmaster's Investment in Facial Recognition Technology", *Paste Magazine*, September 10, 2019, available at: https://www.pastemagazine.com/articles/2019/09/musicians-and-activists-speak-out-against-ticketma.html.
[38] Id.
[39] Dan Reilly "Musicians and Fans Unite to Keep Facial Recognition Tech Out of Concerts", *Fortune Magazine*, September 30, 2019, available at: https://fortune.com/2019/09/30/ban-facial-recognition-live-events-music-festivals-concerts/.
[40] Id.; Ben Kaye "Bonnaroo Electric Forest, Austin City Limits Festivals Say They Won't Use Facial Recognition Tech", *Consequence of Sound*, September 30, 2019, available at: https://consequenceofsound.net/2019/09/bonnaroo-electric-forest-austin-city-limit-festivals-facial-recognition/.
[41] *See* Dan Koeppel, *Casino Hackers*, CNN, Oct. 23, 2006, http://www.cnn.com/2006/TECH/07/13/popsci.gambling/; Stacy Norris, *"... and the Eye in the Sky Is Watching Us*

Nevada, but the technology at that time was not advanced enough to follow a person or to identify faces unless the person looked straight at the camera.[42] By the early 2000s, facial recognition had become a staple at casinos and today the technology has advanced enough that some casino owners boast they can identify someone through facial recognition with 55 percent accuracy, despite the person's face being obscured with "a hat, scarf, and glasses," and sixty-nine percent accuracy "when just glasses were removed."[43]

Concerns Related to Facial Recognition Technology

Technological Limitations

Facial recognition technology is an evolving scientific and diagnostic tool and, therefore is limited in its accuracy and reliability. Factors that can affect proper identification are poor image quality, unusual poses or facial expressions, the age of the photograph, and the race, ethnicity and gender of the person.

Although facial recognition software companies generally claim high accuracy rates, the technology has not been able to overcome its algorithmic biases that tend to misidentify women and people of color in higher proportions. Studies consistently show that facial recognition technologies underperform when aiming to identify people of color, women and non-binary people.[44] This is clearly illustrated in the graph below, which tested the accuracy rates of different

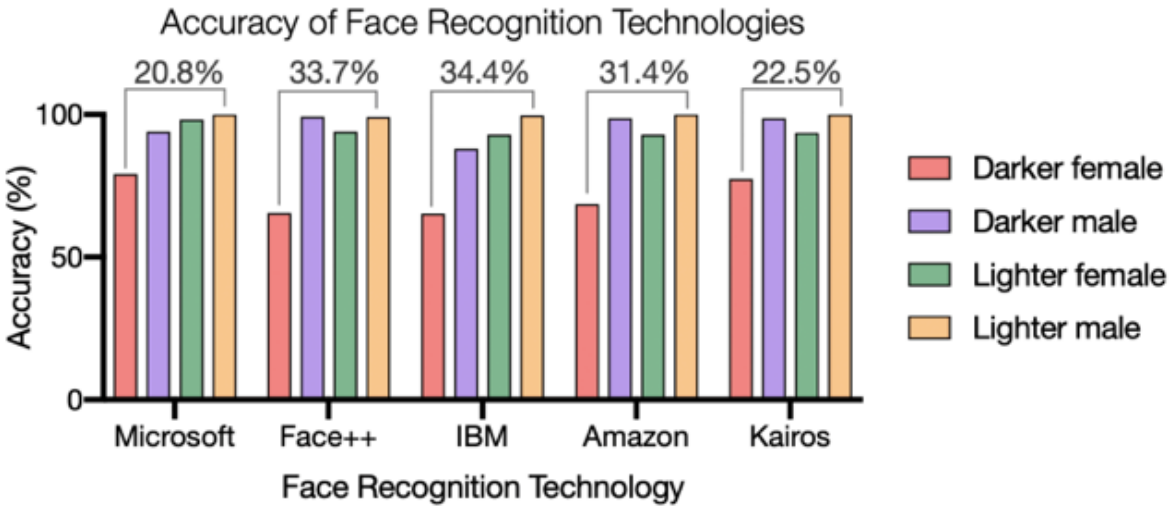
All" - the Privacy Concerns of Emerging Technological Advances in Casino Player Tracking, 9 UNLV GAMING L.J. 269, 291 (2019).

[42] Stacy Norris, *"... and the Eye in the Sky Is Watching Us All" - the Privacy Concerns of Emerging Technological Advances in Casino Player Tracking*, 9 UNLV GAMING L.J. 269, 291 (2019) (citing Jamie Condliffe, *Facial recognition is getting incredibly powerful, and even more controversial*, Bus. Insider, Sept. 8, 2017, http://www.businessinsider.com/facial-recognition-controversy-improvement-2017-9).

[43] Id.

[44] See for example: Drew Harwell "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use", *Washington Post*, December 19, 2019, available at: https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/.

facial recognition software. The results show that facial recognition technologies are far-less accurate when the image is of a dark-skinned female.[45]



Such errors can be particularly damaging for individuals who are mistakenly entered into a criminal database, for example, of supposed shoplifters. This was the alleged case for student Ousmane Bah, who is suing Apple for $1 billion. Bah claims that his name was mistakenly linked to the face of a thief who stole products from an Apple store. The flawed facial recognition hit resulted in the NYPD arriving at Bah's home to arrest him for crimes he had no part in.[46]

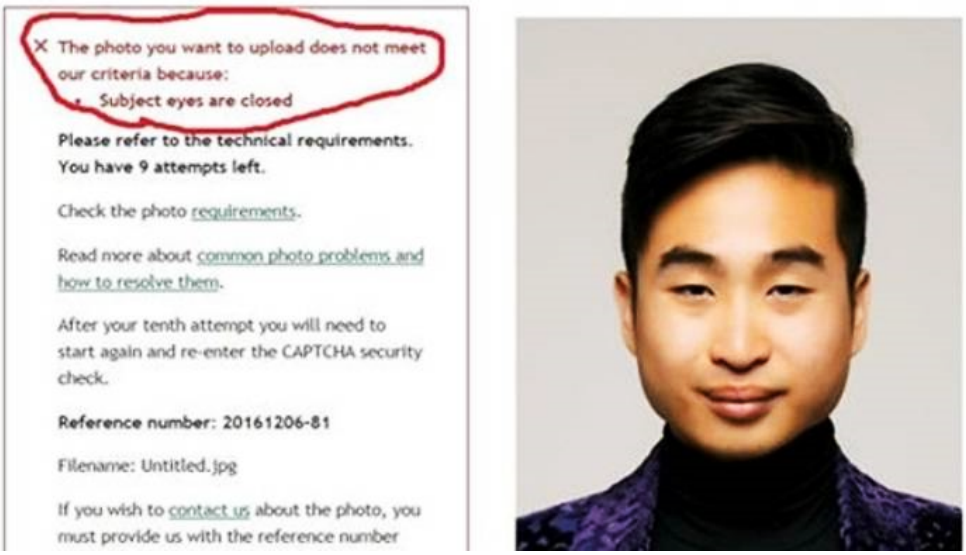
Issues pertaining to the accurate identification of an individual occur when the photos being matched are not taken in a controlled environment or do not necessarily meet the optimal standards for facial recognition software to operate most accurately.[47] In other words, when an individual has his or her face partially obscured, or is facing to the side rather than the front, or the lighting

[45] Alex Najibi "Racial discrimination in face recognition technology", *Harvard University*, October 24, 2020, available at: http://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.
[46] Sigal Samuel "The growing backlash against facial recognition tech", *Vox*, April 27, 2019, available at: https://www.vox.com/future-perfect/2019/4/27/18518598/ai-facial-recognition-ban-apple-amazon-microsoft.
[47] Kristine Hamann & Rachel Smith, *Facial Recognition Technology Where Will It Take Us?*, Crim. Just., Spring 2019, at 9, 10.

is not proper, the verification will be less reliable.[48] Since the outbreak of COVID-19, mask wearing is encouraged, particularly in an indoor/outdoor retail environment or public gathering, throwing into question whether this will further affect the accuracy of this technology. So far, results have been mixed.[49]

Moreover, even uses of facial recognition technology in controlled environments raise significant concerns about accuracy, especially for women, children, African Americans and Asians for whom the existing facial recognition algorithms are known to be less accurate.[50] For example, a New Zealand man of Asian descent had his passport photograph rejected when facial recognition software mistakenly registered his eyes as being closed.[51] The automated system told the 22-year-old engineering student that the photo (illustrated below) was invalid because his eyes were closed, even though they were clearly open.[52]

[48] *See supra,* note 3.
[49] Alfred Ng "Facial recognition designed to detect around face masks is failing, study finds", *CNET*, August 26, 2020, available at: https://www.cnet.com/health/facial-recognition-designed-to-detect-around-face-masks-is-failing-study-finds/.
[50] Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 Conn. L. Rev. 1591, 1596–98 (2017).
[51] James Regan, *New Zealand Passport Robot Tells Applicant of Asian Descent to Open Eyes*, Reuters, December 7, 2016, https://www.reuters.com/article/us-newzealand-passport-error/new-zealand-passport-robot-tells-applicant-of-asian-descent-to-open-eyes-idUSKBN13W0RL.
[52] Id.



Data Breaches and Cyber Security

As the use of facial recognition technology becomes more widespread it can give individuals or businesses the ability to identify almost any person who goes out into public places, surreptitiously or otherwise, tracking movement, location and conduct. This could result in the creation of numerous private and public databases of information, which may be sold, shared or used in ways that the consumer does not necessarily understand or consent to. These databases are vulnerable to security failures and breaches, information leaks by careless or corrupt employees, hackers, or even foreign intelligence agency break-ins.[53]

Biometric information is based on a unique physiological characteristic making it naturally stable and difficult to artificially alter.[54] Biometric information is part of a person's identity. Unlike a password, this information cannot be readily changed. So, for example, if cybercriminals access

[53] Sharon Nakar, Dov Greenbaum "Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy", 23 B.U. J. Sci. & Tech. L. 88, 109 (2017).
[54] *See, e.g.*, Arielle Pardes "Facial Recognition Tech Is Ready for Its Post-Phone Future", *Wired,* September 10, 2018, available at: https://www.wired.com/story/future-of-facial-recognition-technology/.

biometric data — fingerprints, retina, facial or voice — they gain information that can be permanently linked to an identity. Such potential damage could be irreversible.

Biometric data is often collected and stored in large databases that, if not properly protected, are susceptible to hacking. For example, last year, researchers discovered a severe vulnerability in the biometric databases of a company called Suprema, which contained the fingerprints of over one million people, as well as facial recognition information, unencrypted usernames and passwords, and personal information of employees of various clients of the company.[55] These clients included the British Metropolitan Police Service, defense contractors and banks. Suprema describes itself as a "global Powerhouse in biometrics, security and identity solutions," with a product range that "includes biometric access control systems, time and attendance solutions, fingerprint live scanners, mobile authentication solutions and embedded fingerprint modules." [56] Suprema's system was designed to provide centralized control for access to secure facilities like warehouses or office buildings.[57]

Privacy-related Issues

In addition to concerns about data breaches, facial recognition technology also raises a number of privacy concerns. "Unlike other biometric identifiers such as iris scans and fingerprints, facial recognition is designed to operate at a distance, without the knowledge or consent of the

[55] Josh Taylor "Major Breach Found in Biometrics System Used by Banks, UK Police and Defence Firms", *The Guardian*, August 14, 2019, available at: https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms.
[56] Zak Doffman New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report, *Forbes*, August 14, 2019, available at: https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#7309aded46c6; and "Report: Data Breach in Biometric Security Platform Affecting Millions of Users", August 14, 2019, available at: https://www.vpnmentor.com/blog/report-biostar2-leak/.
[57] *See supra*, note 55.

person being identified. Individuals cannot reasonably prevent themselves from being identified by cameras that could be anywhere…."[58]

In New York City, as well as many other municipalities, establishments frequently do not inform customers that facial recognition software is being used, and it is unclear what companies or businesses do with the data once it is collected. Information on customers, their behaviors and their purchasing histories can be valuable, and there have been numerous incidents of companies collecting this information and either selling it to, or having it harvested by third parties, without the knowledge or consent of consumers. The most recent high-profile case where these practices were employed involved Facebook and the political consulting firm Cambridge Analytica that closed its operations in 2018. It was reported that Cambridge Analytica had harvested information from 50 million Facebook profiles to gather data on voters for its clients involved in the pro-Brexit campaign and Donald Trump's election.[59] In a similar situation, consumers of the photo storage application Ever, found their images were being used without their explicit consent. The Ever app was marketed and used a cloud-based photo storage system. However, the company then used these photos to develop their own facial recognition software, which they then sold to law enforcement, the military and private companies.[60]

In Illinois, where legislation mandates that companies inform customers that there is facial recognition technology in use and obtain customers' consent before it can be used on them, a class action lawsuit is being brought against Macy's department stores. According to the complainant,

---

[58] Sharon Nakar, Dov Greenbaum "Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy", 23 B.U. J. Sci. & Tech. L. 88, 96 (2017).
[59] Carole Cadwalladr, *Revealed: 50 Million Facebook Profiles Harvested For Cambridge Analytica In Major Data Breach*, The Guardian, March 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
[60] Olivia Solon and Cyrus Farivar, *Millions of People Uploaded Photos To The Ever App. Then The Company Used Them To Develop Facial Recognition Tools*, NBC News, May 9, 2019, https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371.

Macy's, using a program called Clearview, "is "actively profiting" off information gleaned from the biometric data through improved security and marketing."[61] The Clearview database of faces has been created by the company collating images from people's social media posts, and allows businesses to analyze photos and videos of their customers, captured on in-store surveillance, against the database, in order to identify their customers.[62] According to leaked documents, Walmart, Kohl's, Bank of America, Wells Fargo and a number of government agencies also use Clearview.[63] In November this year, the Los Angeles Police Department banned the use of commercial software, such as Clearview. Now, facial recognition searches can only be run against the database of booking photos, rather than datasets gleaned from social media.[64]

Other government agencies have been accused of mining personal biometric data. For example, earlier this year the *New York Times* reported that Immigration and Customs Enforcement (ICE) used facial recognition software to mine state driver's license databases.[65] ICE is also reportedly using the Clearview software discussed above.[66] Similarly, data from consumer-based surveillance software such as Ring (which uses cameras to monitor a person's doorbell and/or entryway), is also being shared with law enforcement. Ring, which is now owned by Amazon, has partnered with more than 400 local police departments to send requests for footage to Ring users, on behalf of the police. Users can deny the request, but if the request is granted,

---

[61] Robert Channick "Macy's hit with privacy lawsuit over alleged use of controversial facial recognition software", *Chicago Tribune*, August 11, 2020, available at: https://www.chicagotribune.com/business/ct-biz-macys-lawsuit-clearview-facial-recognition-20200811-mstcyf7wufdjvbanpv6ehjtvni-story.html.

[62] Id.

[63] Ryan Mac, Caroline Haskins, and Logan McDonald "Clearview's facial recognition app has been used by the Justice Department, ICE, Macy's, Walmart, and the NBA", *BuzzFeed*, February 27, 2020, available at: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[64] Briana Saks, Ryan Mac, and Caroline Haskins "Los Angeles Police just banned the use of commercial facial recognition", *BuzzFeed*, November 17, 2020, available at: https://www.buzzfeednews.com/article/briannasacks/lapd-banned-commercial-facial-recognition-clearview.

[65] Catie Edmondson, *ICE Used Facial Recognition To Mine State Driver's License Databases*, New York Times, July 7, 2019, https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html?searchResultPosition=12.

[66] *See supra,* note 63.

police are able to obtain consumer-recorded video footage, without the need for a warrant. In exchange, the police departments promote Ring as an important security device.[67] Indeed, at least one police department in California has offered the Ring devices as a reward to members of the public, in lieu of cash, for information on crimes.[68]

The ubiquity of facial recognition technology also raises serious concerns over where a person can expect a degree of privacy and anonymity. To demonstrate the ease with which this technology can be employed, the *New York Times* conducted its own facial recognition project of people in Bryant Park during an afternoon. They utilized footage taken from three cameras that publicly stream the happenings of the park and ran the images through facial recognition software that cost less than $100. Through this process, the team was able to detect 2,750 faces from a nine-hour period and, using a database created from publicly available photos, they were able to match identities.[69] While being identified as being in Bryant Park one lunchtime might seem innocuous enough, the power of this technology has potentially dangerous ramifications. For instance, in Hong Kong, facial recognition has been employed by rival sides to identify both protesters and police.[70] Meanwhile, in the United States, toy store Toys "R" Us is reportedly using the technology in their stores, although they claim that the algorithm is capable of excluding children.[71]

Other Jurisdictions

[67] Louise Matsakis "The Ringification of suburban life", *Wired,* September 26, 2019, https://www.wired.com/story/ring-surveillance-suburbs/.
[68] Louise Matsakis *"Cops Are Offering Ring Doorbell Cameras in Exchange For Info", Wired,* September 2, 2019, https://www.wired.com/story/cops-offering-ring-doorbell-cameras-for-information/.
[69] Sahil Chinoy "We built an 'unbelievable' (but legal) facial recognition machine", *New York Times*, April 16, 2019, https://www.nytimes.com/interactive/2019/04/16/opinion/facial-recognition-new-york-city.html.
[70] Paul Mozur, *In Hong Kong Protests, Faces Become Weapons*, New York Times, July 26, 2019, https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html?searchResultPosition=16.
[71] Louis Matsakis "Toys "R" Us is back—Now with more surveillance!", *Wired*, November 12, 2020, available at: https://www.wired.com/story/toys-r-us-surveillance/.

To combat some of the concerns regarding the use of facial recognition technology, jurisdictions across the country have enacted legislation to regulate it. Illinois' Biometric Information Privacy Act, a forerunner in governing this technology, has been in place for more than ten years, but more states and cities are looking to legislate on the issue and there are also numerous proposed bills at the federal level.[72]

Portland, OR

In September 2020, Portland became the first US jurisdiction to ban private entities' use of facial recognition technology in places of public accommodation.[73] The legislation also allows a private right of action, but the ban is limited to technology related to facial recognition, and not other biometric identifiers.[74] Portland also passed a separate ordinance to ban the use of the technology by local government agencies.

Illinois

In 2008, Illinois became the first jurisdiction in the country to enact legislation related to biometric data use. Under the Illinois Biometric Information Privacy Act (BIPA), any private entity that collects biometric identifier information must first provide a written disclosure and

[72] For example, Arizona, Massachusetts, West Virginia, South Carolina, Maryland, Utah, and New Jersey all have bills related to biometric data, but as of early October 2020, none have passed. There are also several jurisdictions in Massachusetts that have banned the use of facial recognition technology by local government (see: Amba Kak "Regulating Biometrics: Global Approaches and Urgent Questions", *AI Now Institute,* September 2020, available at: https://ainowinstitute.org/regulatingbiometrics.pdf, p. 90.

[73] Hunton Andrews Kurth "Portland, Oregon Becomes First Jurisdiction in U.S. to Ban the Commercial Use of Facial Recognition Technology", *National Law Review*, September 10, 2020, available at: https://www.natlawreview.com/article/portland-oregon-becomes-first-jurisdiction-us-to-ban-commercial-use-facial#:~:text=On%20September%209%2C%202020%2C%20Portland,including%20stores%2C%20restaurants%20and%20hotels

[74] Id.

obtain a release from any individuals whose biometric information is being collected.[75] The law also prohibits the sale of biometric information. BIPA also includes a private right of action.[76]

Texas

The Texas law prohibits the collection of an individual's biometric identifiers for a commercial purpose, unless the individual is first informed and consents.[77] Texas law also requires consent for the sale or disclosure of an individual's biometric identifiers, and entities must use reasonable care in storing [biometric data] and shall destroy the biometric identifier within a reasonable time."[78] However, Texas does not offer a private right of action and only the Attorney General can enforce violations of the law.[79]

California

California's Consumer Privacy Act (CCPA), which went into effect at the beginning of this year, takes a broader definition of biometric data to include "keystroke and gait patterns as well as sleep, health, and exercise data that contain identifying information."[80] However, the private right of action under CCPA does not cover biometric data.[81]

In terms of disclosures, the CCPA grants a 'right to know' so that a person "may request that businesses disclose…what personal information they have collected, used, shared, or sold

[75] 740 Ill. Comp. Stat. Ann. 14/15
[76] *Id.* at 14/20
[77] Tex. Bus. & Com. Code Ann. § 503.001 (West)
[78] Id.
[79] Id.
[80] California Consumer Privacy Act of 2018, §1798.140 (b).
[81] Molly K. McGinley "The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States", *National Law Review*, March 25, 2019, available at: https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states.

about you, and why they collected, used, shared, or sold that information."[82] It also allows consumers to request deletion of information and opt-out of the sale of their data to third-parties.[83]

Washington

The Washington law[84] prohibits both companies and individuals "from entering biometric data into a database without providing notice, gaining consent and providing a mechanism for preventing the subsequent use of the biometric data for a commercial purpose".[85] Notably, unlike the laws in the above states, under Washington's legislation the definition of "biometric identifier" excludes facial recognition data, and instead is limited to "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual."[86]

COVID-19 and Biometric Information

While biometric technology itself has been around for some time, the COVID-19 pandemic has given rise to new applications for the purpose of identifying and tracking individuals for health screening purposes. The HealthPass by CLEAR is one such example. Users download the application, verify their identity through biometric identifiers (such as a fingerprint and iris scan),[87] and then input any health related data, such as COVID-19 lab tests, or self-reported symptoms. Employers or other establishments such as airports or businesses serving customers, might then

[82] California Attorney General Xavier Becerra "California Consumer Privacy Act (CCPA)", available at: https://oag.ca.gov/privacy/ccpa#sectionc.
[83] *Id.*
[84] Wash. Rev. Code Ann. §§ 19.375.010- 19.375.040 (West)
[85] "State Biometric Privacy Legislation: What You Need to Know", *Thompson Hine,* September 5, 2019, available at: https://www.thompsonhine.com/publications/state-biometric-privacy-legislation-what-you-need-to-know#:~:text=Washington%20enacted%20biometric%20privacy%20protections,data%20for%20a%20commercial%20purpose.
[86] NYC Bar Association "Power, pervasiveness and potential", August 2020, p. 15.
[87] CLEAR "How it works", available at: https://www.clearme.com/how-it-works.

expedite users' entry into a facility. At the point of entry, users may open an app, verify their identity in some manner, and possibly have their temperature taken through a scan.[88] In New York City, businesses already using HealthPass include "the Related Companies, Cushman & Wakefield, Deloitte, NBC Universal, the New York Mets and Danny Meyer's Union Square Hospitality Group."[89] The restaurant group Founder's Table, which runs restaurant chains including Chopt and Dos Toros, are requiring their staff to use the app. The employees are required to take a health survey each day to enter their jobsite.[90] The World Economic Forum, together with the Commons Project, is also currently developing an app where users can store their COVID-19-related health information, for verification at airports and other travel hubs. Once publicly available, app users may be able to upload their COVID-19 health data onto the app, regardless of the country in which they took the tests, and have the results verified, according to the standards of the country of entry.[91]

However, unlike commercial establishments that surreptitiously collect biometric information themselves from consumers who access their goods or services, these COVID-19 applications are downloaded and consented to by the user themselves.

III. LEGISLATIVE ANALYSIS

This bill addresses the increased collection and use of biometric identifier information, such as the use of facial recognition technology, by commercial establishments to track consumer activity. This bill would require commercial establishments to post signage that notifies customers

[88] CLEAR "Health Pass", on file.
[89] *The Real Deal* "Related, Cushman & Wakefield use new app to screen workers for Covid", October 28, available at: https://therealdeal.com/2020/10/28/related-cushman-wakefield-use-new-app-to-screen-workers-for-covid/.
[90] Jessica Puckett "Clear goes beyond airports with its COVID-19 screening service", *Condé Nast Traveler,* July 31, 2020, available at: https://www.cntraveler.com/story/clear-goes-beyond-airports-with-its-covid-19-screening-service.
[91] CommonPass, available at: https://commonpass.org.

if the establishment "collects, retains, converts, stores or shares" biometric identifier information used to identify individuals, such as scans of customer faces, irises, or fingerprints. Commercial establishments are defined as "a place of entertainment, a retail store, or a food and drink establishment." The bill also makes it unlawful "to sell, lease, trade, share in exchange for anything of value or otherwise profit" from the exchange of customer's biometric identifier information that these establishments have used to identify individuals.

The bill provides for a private right of action that allows for judgments of $500 for failing to post signage or negligently selling/sharing covered biometric information and $5,000 for the intentional or reckless sale of such biometric information. Prior to filing an action for a violation of the signage requirement, a plaintiff must provide the commercial establishment with written notice of the violation. The commercial establishment must provide a written response within 30 days stating the violation has been cured, otherwise the plaintiff may proceed with filing an action. The plaintiff is not required to provide written notice for violations of the prohibition on the sale of biometric identifier information.

This bill does not apply to governmental entities. The requirement to post signs does not apply to financial institutions, which already adhere to various disclosure requirements in terms of the collection of personal information, or to commercial establishments that collect biometric information only through photographs or video recordings that do not utilize automated or assisted processes to identify individuals, and which do not share photos or video with any entity other than law enforcement. The bill requires the Department of Consumer and Worker Protection to create rules regarding the posting of the required signage. It also requires the Chief Privacy Officer, in conjunction with other relevant City agencies, to conduct outreach and education to affected commercial establishments.

This local law takes effect 180 days after it becomes law.

Int. No. 1170-A

By Council Members Torres, Rosenthal, Rivera, Moya, Rose, Cornegy, Louis, Gibson, Kallos, Menchaca and Ayala

A Local Law to amend the administrative code of the city of New York, in relation to requiring businesses to notify customers of the use of biometric identifier technology and prohibiting the sale of biometric identifier information

Be it enacted by the Council as follows:

Section 1. Title 22 of the administrative code of the city of New York is amended by adding a new chapter 12 to read as follows:

CHAPTER 12

BIOMETRIC IDENTIFIER INFORMATION

§ 22-1201 Definitions.

§ 22-1202 Collection, use, and retention of biometric identifier information.

§ 22-1203 Private right of action.

§ 22-1204 Applicability.

§ 22-1205 Outreach and education.

§ 22-1201 Definitions. As used in this chapter, the following terms have the following meanings:

Biometric identifier information. The term "biometric identifier information" means a physiological or biological characteristic that is used by or on behalf of a commercial establishment, singly or in combination, to identify, or assist in identifying, an individual, including, but not limited to: (i) a retina or iris scan, (ii) a fingerprint or voiceprint, (iii) a scan of hand or face geometry, or any other identifying characteristic.

Commercial establishment. The term "commercial establishment" means a place of entertainment, a retail store, or a food and drink establishment.

Consumer commodity. The term "consumer commodity" means any article, good, merchandise, product or commodity of any kind or class produced, distributed or offered for retail sale for consumption by individuals, or for personal, household or family purposes.

Customer. The term "customer" means a purchaser or lessee, or a prospective purchaser or lessee, of goods or services from a commercial establishment.

Financial institution. The term "financial institution" means a bank, trust company, national bank, savings bank, federal mutual savings bank, savings and loan association, federal savings and loan association, federal mutual savings and loan association, credit union, federal credit union, branch of a foreign banking corporation, public pension fund, retirement system, securities broker, securities dealer or securities firm, but does not include a commercial establishment whose primary business is the retail sale of goods and services to customers and provides limited financial services such as the issuance of credit cards or in-store financing to customers.

Food and drink establishment. The term "food and drink establishment" means an establishment that gives or offers for sale food or beverages to the public for consumption or use on or off the premises, or on or off a pushcart, stand or vehicle.

Place of entertainment. The term "place of entertainment" means any privately or publicly owned and operated entertainment facility, such as a theater, stadium, arena, racetrack, museum, amusement park, observatory, or other place where attractions, performances, concerts, exhibits, athletic games or contests are held.

Retail store. The term "retail store" means an establishment wherein consumer commodities are sold, displayed or offered for sale, or where services are provided to consumers at retail.

§ 22-1202 Collection, use, and retention of biometric identifier information. a. Any commercial establishment that collects, retains, converts, stores or shares biometric identifier information of customers must disclose such collection, retention, conversion, storage or sharing, as applicable, by placing a clear and conspicuous sign near all of the commercial establishment's customer entrances notifying customers in plain, simple language, in a form and manner prescribed by the commissioner of consumer and worker protection by rule, that customers' biometric identifier information is being collected, retained, converted, stored or shared, as applicable.

b. It shall be unlawful to sell, lease, trade, share in exchange for anything of value or otherwise profit from the transaction of biometric identifier information.

§ 22-1203 Private right of action. A person who is aggrieved by a violation of this chapter may commence an action in a court of competent jurisdiction on his or her own behalf against an offending party. At least 30 days prior to initiating any action against a commercial establishment for a violation of subdivision a of section 22-1202, the aggrieved person shall provide written notice. to the commercial establishment setting forth such person's allegation. If, within 30 days, the commercial establishment cures the violation and provides the aggrieved person an express written statement that the violation has been cured and that no further violations shall occur, no action may be initiated against the commercial establishment for such violation. If a commercial establishment continues to violate subdivision a of section 22-1202, the aggrieved person may initiate an action against such establishment. No prior written notice is required for actions alleging a violation of subdivision b of section 22-1202. A prevailing party may recover:

1. For each violation of subdivision a of section 22-1202, damages of $500;

2. For each negligent violation of subdivision b of section 22-1202, damages of $500;

3. For each intentional or reckless violation of subdivision b of section 22-1202, damages of $5,000;

4. Reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

5. Other relief, including an injunction, as the court may deem appropriate.

§ 22-1204 Applicability. a. Nothing in this chapter shall apply to the collection, storage, sharing or use of biometric identifier information by government agencies, employees or agents.

b. The disclosure required by subdivision a of section 22-1202 shall not apply to:

1. Financial institutions.

2. Biometric identifier information collected through photographs or video recordings, if: (i) the images or videos collected are not analyzed by software or applications that identify, or that assist with the identification of, individuals based on physiological or biological characteristics, and (ii) the images or video are not shared with, sold or leased to third-parties other than law enforcement agencies.

§ 22-1205 Outreach and education. The chief privacy officer shall conduct or facilitate, with any other relevant agency or office, outreach and education efforts, through guidance posted on city websites or through such other means as may be feasible, to inform commercial establishments likely to be affected by this chapter about its requirements.

§ 2. This local law takes effect 180 days after it becomes law.

SIL/BAM
LS #5625
12/2/2020